

**IN THE UNITED STATES DISTRICT COURT FOR**  
**THE NORTHERN DISTRICT OF GEORGIA**  
**ATLANTA DIVISION**

---

**DONNA CURLING, et al.**

**Plaintiff,**

**vs.**

**BRAD RAFFENSPERGER, et al.**

**Defendant.**

---

**CIVIL ACTION FILE NO.:  
1:17-cv-2989-AT**

**DECLARATION OF DUNCAN A. BUELL**

DUNCAN A. BUELL ("Declarant") hereby declares as follows:

1. I am a retired professor of Computer Science and Engineering at the University of South Carolina, Columbia, and have been teaching one course a semester as a visitor at Denison University in Granville, Ohio.

2. I am writing to express my strong support for the Plaintiffs' request to promptly have Professor Alex Halderman's redacted report on the Dominion voting system made public and available.

**Qualifications and Relevant Employment History**

3. In 1971, I earned a B.S. in Mathematics from the University of Arizona. The following year, I earned an M.A. in Mathematics from the University of Michigan. In 1976, I earned a doctorate in Mathematics, with an emphasis in number theory, from

the University of Illinois at Chicago. A copy of my resume is available on my university website at <http://www.cse.sc.edu/~buell>.

4. Prior to moving into my position at the University of South Carolina, I was employed for just under 15 years (with various job titles and duties) at the Supercomputing Research Center (later named the Center for Computing Sciences) of the Institute for Defense Analyses, a Federally Funded Research and Development Center (FFRDC) supporting the National Security Agency. Our mission at SRC/CCS was primarily to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA. While at IDA, I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then “the largest single computation ever made” in the U.S. intelligence community. While at IDA, all our publications and public presentations were required to be vetted by NSA, and they were frequently edited if those who did the vetting felt that the material as written crossed the line and needed to be redacted. Although the *nature* of the sensitivity of that information is somewhat different from the information in Halderman’s original and redacted reports, the *process* of evaluating risk versus reward seems to me to very similar, and I am very familiar with the ways in which intelligence organizations evaluate risk versus reward in dealing whether information, especially about vulnerabilities in software, is, or should be, made public.

5. From 2000 until my retirement on 1 January 2021, I was a Professor in the Department of Computer Science and Engineering at the University of South Carolina.

From 2000 to 2009, I served as Chair of that department. During 2005-2006, I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina.

6. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to an endowed professorship, the NCR Chair in Computer Science and Engineering at the University of South Carolina.

7. My current research interests include electronic voting systems, digital humanities, high performance computing applications, parallel algorithms and architecture, computer security, computational number theory, and information retrieval. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured on each of these topics.

8. In March 2019 I was nominated by the county legislative delegation and then appointed by Governor Henry McMaster to the Board of Voter Registration and Elections of Richland County, South Carolina. I held this position until March 2021, when I resigned because I was moving in April 2021 from South Carolina to Ohio.

### **Basis for My Opinions**

9. I base the opinions in this declaration on my knowledge, skill, training, education, research, and experience: I have been programming computers for more than 50 years and was employed as a computer scientist for more than 40 years, including the 15 years I spent at IDA SRC/CCS, which involved extensive dealing with highly classified technical material as well as “sanitizing” material for wider availability.

10. I have signed the Protective Order regarding the original 1 July 2021 Halderman report. I have read that report, and the redacted version, and the CISA report report validating Professor Halderman's findings. I believe the redacted version is an appropriate redaction of the original report. I believe that Professor Halderman has in the original report listed obvious possible vulnerabilities and the details of how those could be exploited. I do *not* believe that listing obvious possible vulnerabilities is sensitive material to be withheld from election officials, their advisers, and the public. I *do* believe that the details of the exploitations of those vulnerabilities, done in the unredacted report, is sensitive and should be kept as closely held as possible.

**My Opinion: Releasing the Redacted Report Is Crucial to Securing Elections**

11. The Dominion system is used across the country for elections. The entire system has been copied (at least from Coffee County, if not also from elsewhere) and made available to numerous unauthorized and unknown actors. We don't know who now has the software of the Dominion system, and the redacted report (and by now perhaps the original report), and could thus launch compromises to integrity from inside or outside election offices. The *prudent* response to this threat is to make the redacted report available, so that election officials across the country would know what the vulnerabilities are and take steps to mitigate the threats. Their technical advisers, as well as election oversight groups, need to have access to that information. Ignorance on the part of those we trust to run good elections endangers those elections nationally.

12. Importantly, the release should go beyond just election and government officials. There is a national shortage of computer security experts, and we cannot expect

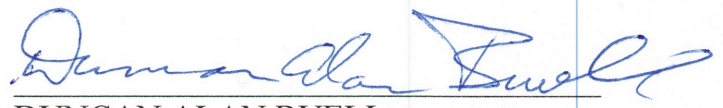
all the government bodies that manage elections will have sufficient in-house expertise – at government salaries -- in order to mitigate the vulnerabilities. (I remember that there are counties in South Carolina, for example, where the elections office gets a fraction of the time of the one county IT employee. I would not expect that this situation is confined to South Carolina; there are likely counties in Georgia and elsewhere with the same limited availability of expertise.) One would then have to expect that the redacted report would need to be distributed by election officials to companies that specialized in computer security as part of a procurement process. I know from my time at IDA that, given the U. S. government's concentration in the DC area, there are many companies that can readily do classified work because there's enough government business that the companies can afford to hire and clear all their employees for access to restricted material. This will not be the case in rural Georgia or elsewhere in the U.S. With this kind of expectation, then, it seems that release to the public would minimize the complexity of local officials' plans for mitigating the vulnerabilities and would contribute to public confidence in elections by increasing the transparency of the process.

13. Finally, state and county legislative and regulatory bodies, and their advisers, need access to the information as they consider voting system requirements and regulations, and even future voting system purchases or upgrades. Those bodies that purchase equipment, set policy and procedures, and such, need to be informed as to what specific questions to ask of vendors regarding vulnerabilities known (almost certainly by some bad actors) to have existed in previous versions of the election system. Responsible disclosure of the existence of vulnerabilities allows those who use systems with those

vulnerabilities to ask direct questions of the vendors of those systems, and it allows users (in this case election officials, and those involved in procurement of equipment and policies for its use) and advocates to focus attention on whether or not the vendors have fixed the defects. This kind of responsible disclosure enhances security.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, 15 May, 2023.

  
DUNCAN ALAN BUELL